

CLAIM 1

Claim 1 recites a method for:

selectively enforcing a security policy in a network, the method comprising the computer-implemented steps of:
creating and storing one or more access controls in a policy enforcement point device that controls access of clients to the network, wherein each of the access controls specifies that a named abstract group is allowed access to a particular resource;
receiving, from an external binding process, a binding of a network address to an authenticated user of one of the clients for which the policy enforcement point controls access to the network;
updating the named group to include the bound network address of the authenticated user at the policy enforcement point; and
permitting a packet flow originating from the network address to pass from the policy enforcement point into the network only if the network address is in the named group identified in one of the access controls that specifies that the named group is allowed access to the network (emphasis added).

Reid and *Ray* do not teach, alone or in combination, all the elements of Claim 1. The Office Action asserts that the steps of “receiving, from an external binding process, a binding of a network address to an authenticated user of one of the clients for which the policy enforcement point controls access to the network; updating the named group to include the bound network address of the authenticated user at the policy enforcement point;” is expressly described in *Ray* (Col. 4, line 65 to col. 5, line 31; and col. 6, line 66 to col. 7, line 6). The Applicant respectfully submits that the text cited by the Office Action does not teach “receiving...a binding of a network address to an authenticated user” and “updating the named group...at the policy enforcement point,” as required by Claim 1.

The text cited for “receiving...a binding of a network address to an authenticated user” simply describes a method for a network device receiving a network address from a network server once the network device is added to a network (Col. 4, line 65 to col. 5, line 31). *Ray* makes no mention of “an authenticated user,” or anything relating to authentication, as required by Claim 1. Further, a binding of an authenticated user to a network address is not the same as a

network address alone. Therefore, nothing in *Ray* teaches nor suggests the step of “receiving...a binding of a network address to an authenticated user.”

The text in *Ray* cited for the step of “updating the named group to include the bound network address of the authenticated user at the policy enforcement point” simply teaches that a network device, once it has received a network address, notifies a gateway address server, which saves the network address and subsequently informs other network devices of the newly assigned network address (Col. 6, line 66 to col. 7, line 6). Even assuming that the gateway address server of *Ray* is equivalent to the policy enforcement point of Claim 1, as the Office Action alleges, no updating of a named group is occurring. In fact, nothing in *Ray* mentions anything about groups, much less updating a named group. Therefore, it is impossible for *Ray* to teach, much less suggest the step of “updating the named group to include the bound network address of the authenticated user at the policy enforcement point.”

The Office Action also asserts that the step of “permitting a packet flow originating from the network address to pass from the policy enforcement point into the network only if the network address is in the named group identified in one of the access controls that specifies that the named group is allowed access to the network” is expressly described in *Reid* (Col. 6, lines 21-31). The text cited by Office Action does not teach “permitting a packet flow...if the network address is in the named group identified in one of the access controls.” *Reid* teaches that a connection request to a group can be checked against an access rule according to the connection’s user, group, or IP address (Col. 6, lines 23-25). *Reid* neither expressly nor inherently teaches anything about “permitting packet flow...**if the network address is in the named group identified in one of the access controls,**” as required by Claim 1. Nothing in *Reid* teaches nor suggests the feature of determining whether a network address **is in a named**

group, much less that the “network address is in the named group identified in one of the access controls.”

In view of the foregoing, Claim 1 includes at least three limitations that are not taught or suggested by *Ray* and *Reid*. Also, the Office Action does not allege 1) that *Reid* teaches the elements of Claim 1 that are missing from *Ray* and 2) that *Ray* teaches the elements of Claim 1 that are missing from *Reid*. Thus, *Ray* and *Reid* fail to disclose alone, or in combination, all the elements of the Claim 1. Claim 1 is therefore patentable over *Reid* and *Ray*.

CLAIMS 2-20, AND 23-24

Claims 2-6 all depend from Claim 1 and include all of the limitations of Claim 1. Therefore, Claims 2-6 are patentable over *Reid* and *Ray* for at least the reasons set forth herein with respect to Claim 1. Furthermore, Claims 2-6 recite additional limitations that independently render them patentable over *Reid* and *Ray*.

Claims 13-18 include limitations similar to Claims 1-6, except in the context of computer-readable media. Therefore, Claims 13-18 are patentable over *Reid* and *Ray* for at least the reasons set forth herein with respect to Claims 1-6.

Claims 7-12 include the same limitations of Claims 1-6 that are discussed above, and thus Claims 7-12 are patentable over *Reid* and *Ray* for the reasons set forth herein with respect to Claims 1-6.

Claims 19 and 20 include the same limitations of Claim 1 that are discussed above, and thus Claims 19 and 20 are patentable over *Reid* and *Ray* for the reasons set forth herein with respect to Claim 1.

In view of the foregoing, reconsideration and withdrawal of the rejection of Claims 1-20 and 23-24 is respectfully requested.

B. CLAIM 21

Claim 21 is rejected under 35 U.S.C. § 103(a) as being unpatentable over *Reid* and *Ray*, and further in view of the article by *Stewart*. The rejection is respectfully traversed.

Claim 21 is dependent upon Claim 1 and thus includes each and every feature of Claim 1. Also, the Office Action does not allege that *Stewart* teaches the elements of Claim 1 that are missing from *Reid* and *Ray*. Thus, *Stewart* fails to disclose alone, or in combination with *Reid* and *Ray*, all the elements of the Claim 21. Claim 21 is therefore allowable for the reasons given above for Claim 1. Therefore, it is respectfully submitted that Claim 21 is allowable for the reasons given above with respect to Claim 1.

C. CLAIM 22

Claim 22 is rejected under 35 U.S.C. § 103(a) as being unpatentable over *Reid* and *Ray*, and further in view of *Stevens*. The rejection is respectfully traversed.

Claim 22 is dependent upon Claim 1 and thus includes each and every feature of Claim 1. Also, the Office Action does not allege that *Stevens* teaches the elements of Claim 1 that are missing from *Reid* and *Ray*. Thus, *Stevens* fails to disclose alone, or in combination with *Reid* and *Ray*, all the elements of the Claim 22. Claim 22 is therefore allowable for the reasons given above for Claim 1. Therefore, it is respectfully submitted that Claim 22 is allowable for the reasons given above with respect to Claim 1.

II. CONCLUSIONS & MISCELLANEOUS

For the reasons set forth above, it is respectfully submitted that all of the pending claims are now in condition for allowance. Therefore, the issuance of a formal Notice of Allowance is believed next in order, and that action is most earnestly solicited.

The Examiner is respectfully requested to contact the undersigned by telephone if it is believed that such contact would further the examination of the present application.

A petition for extension of time, to the extent necessary to make this reply timely filed, is
hereby made. If applicable, a law firm check for the petition for extension of time fee is enclosed
herewith. If any applicable fee is missing or insufficient, throughout the pendency of this
application, the Commissioner is hereby authorized to any applicable fees and to credit any
overpayments to our Deposit Account No. 50-1302.

Respectfully submitted,

HICKMAN PALERMO TRUONG & BECKER LLP

Dated: July 28, 2004



Christopher J. Palermo
Reg. No. 42,056

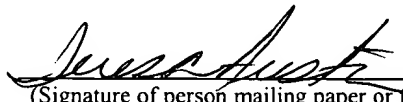
1600 Willow Street
San Jose, California 95125-5106
Telephone No.: (408) 414-1202
Facsimile No.: (408) 414-1076

CERTIFICATE OF MAILING

I hereby certify that this paper or fee is being deposited with the United States Postal Service under 37 CFR 1.8 on the date indicated below and is addressed to the Mail Stop Amendment, Commissioner for Patents, P. O. Box 1450, Alexandria, Virginia 22313-1450

Teresa Austin

(Typed or printed name of person mailing paper or fee)



(Signature of person mailing paper or fee)

Dated: July 28, 2004